1 The Foundations: Logic and Proofs

1.1 Propositional Logic

1. a proposition is a declarative sentence that is either true (T) or false (F), but not both.

2. a sentence with a variable can be turned into a proposition if a value is assigned to the variable

3. a propositional variable is a variable that can be turned into a proposition by assigning value to it (Ex: propositional variables: $P(x) : x > 0$. The proposition $P(-3) : -3 > 0$ is false)

4. propositional calculus or propositional logic is the area of logic that deals with propositions

5. compound propositions are new propositions obtained from already existing ones, using logical operators (or connectives: NOT, AND, OR, XOR, IF...THEN, IFF)

6. in deciding whether a sentence that involves a variable is T or F, we use fixed time, place and particular people

7. truth tables are tables that display all the possible choices for the propositions. For example, if only one proposition is involved, there are only two choices: T or F. If two propositions are involved, there are four choices to consider: both T, both F, first T and second one F, or first F and second one T (see tables page 4)

8. truth tables for the negation of p ($\neg p$), p and q ($p \wedge q$), p or q ($p \vee q$), p exclusive or q ($p \oplus q$), implication ($p \rightarrow q$), biconditional ($p \leftrightarrow q$)

9. in an implication ($p \rightarrow q$), p is the hypothesis and q is the conclusion

10. the converse of ($p \rightarrow q$) is $q \rightarrow p$

11. the inverse of ($p \rightarrow q$) is $\neg p \rightarrow \neg q$

12. the contrapositive of ($p \rightarrow q$) is $\neg q \rightarrow \neg p$

13. precedence of logical operators: $\neg$; then $\vee$ and $\wedge$, and then $\rightarrow$ or $\leftarrow$ or $\leftrightarrow$

14. a boolean variable is a variable that is either T or F, so it could be regarded as a "1 or 0 type" of variable

15. a bit string is a sequence of zero or more bits

16. the length of a bit string is the number of bits in the string

17. OR, AND, and XOR can be done bit wise instead of using T and F

1.2 Propositional Equivalences

1. tautology is a compound proposition that is always true
2. contradiction is a compound proposition that is always false
3. contingency is a compound proposition that is neither always false nor always true
4. p and q are logically equivalent ($p \equiv q$) if $p \leftrightarrow q$ is a tautology.
5. $p \equiv q$ is not a compound proposition, but rather the statement that asserts that $p \leftrightarrow q$ is a tautology.
6. $\equiv$ is a symbol that is not a connective like $\vee, \wedge, \neg ...$
7. In proving that two statements are logically equivalent, one can use:
   - truth tables
   - using the logical equivalences already established in Table 6 (one more: $p \rightarrow q \equiv \neg p \vee q$)
8. De Morgan's laws–they help negate compound propositions

1.3 Predicates and Quantifiers

1. predicate logic is the area of logic that deals with predicates (and quantifiers)
2. the predicate is the property that the subject of the statement can have. Example of a predicate: "is an integer"
3. the propositional function P at x is the statement that involves the variable x, that will be a proposition when x is assigned a value. For example: $P(x) : x$ is an integer.
4. propositional functions may have more than one variable, for example $P(x, y, z)$
5. a quantifier expresses the extend to which the predicate is true over a range of values, and it helps create a proposition from propositional function.
   Example: $\forall x \in \mathbb{Z}, x^2 \in \mathbb{N}$
6. the quantifiers are:
   - the universal quantifier: $\forall x$. This means that for all values of x $P(x)$ is true. Example: $\forall x \in \mathbb{N}, x^3 \geq 0$.
   - existential quantifier: $\exists x$. This means that there is at least one value of x so that $P(x)$ is true. Example: $\exists x \in \mathbb{N}, x^3 \geq 10$.
   - uniqueness quantifier: $\exists !$. This means that there is *exactly* one value of x so that $P(x)$ is true. Example: $\exists ! x \in \mathbb{N}, x^3 = 0$.

7. a counterexample to $\forall x, P(x)$ is an element x for which $P(x)$ is false. For example, let $P(x) : \forall x \in \mathbb{N}, x^3 \geq 10$. A counterexample is the value $x = 0$, or $x = 2$.

8. note that "$\forall x \in A$, $P(x)$" is the same as saying " if $x \in A$, then $P(x)$", so it is an implication

9. when we have $\forall x \in A$, $P(x)$ or $\exists x \in A$, $P(x)$, then we assume that there is some value in the domain. What that says is that $\forall x \in A$, $P(x)$ is true if the set A is empty as well, but we generally assume that A is nonempty (however one should check if A is empty or not).

10. quantifiers have higher precedence than all logical operators from propositional calculus. Example: $\forall x P(x) \vee Q(x)$ means $\Big(\forall x P(x)\Big) \vee Q(x)$ and not $\forall x \Big(P(x) \vee Q(x)\Big)$

11. if a quantifier is used on a variable x, we say that x is bound, and it is free otherwise

12. two statements involving quantifiers and connectives are logically equivalent iff they have the same truth values for the same predicates and variables that are substituted in (any value of the domain could be used).

13. **Negating quantifiers:**

    - $\neg\Big(\forall x P(x)\Big) \equiv \exists x \neg P(x)$ $\Big($or $\neg\Big(\forall x \in A,\ P(x)\Big) \equiv \exists x \in A,\ \neg P(x)\Big)$
    - $\neg\Big(\exists x P(x)\Big) \equiv \forall x \neg P(x)$ $\Big($or $\neg\Big(\exists x \in A,\ P(x)\Big) \equiv \forall x \in A,\ \neg P(x)\Big)$

    For example: $\neg(\forall x \geq 0, x^2 \geq 1)$ is $\exists x \geq 0, x^2 < 1$.

1.4 Nested Quantifiers

1. in this section we combine more than one quantifier in the same mathematical statement

2. $\forall x \exists y, P(x, y)$ is the same as $\forall x, Q(x, y)$ where $Q(x, y) : \exists y, P(x, y)$

3. the order of the quantifiers is important: $\forall x \exists y, P(x, y) \not\equiv \exists y \forall x, P(x, y)$

4. Generally: if the two symbols are the same (such as $\forall x \forall y, P(x, y)$ or $\exists x \exists y, P(x, y)$) then the order of the variables doesn't matter. It is commonly written as: $\forall x \forall y, P(x, y) \equiv \forall x, y, P(x, y)$.

5. However, if the two symbols are not the same (such as $\forall x \exists y, P(x, y)$ or $\exists x \forall y, P(x, y)$) then the order matters, and the two propositions have different meanings (see table 1 page 53)

6. $\forall x \exists y, P(x,y)$ means that no matter what x you choose, there is y that makes $P(x,y)$ true (most of the times y depends on x). Example: $\forall x \exists y, x + y = 0$. To see this, let $y = -x$.

7. now, $\exists x \forall y, P(x,y)$ means that you could find some x, such that no matter what y you choose (this y cannot depend on x, it should be any value y) $P(x,y)$ is true. Example: $\exists x \forall y, x + y = 0$. This is not true, because you can always find some y that makes it false. However, the proposition $\exists x \forall y (y \neq 0), \frac{x}{y} = 0$ is true.

8. additive inverse of x is $-x$ (so that adding them up you get 0)

9. multiplicative inverse of x is $\frac{1}{x}$ (so that when you multiply them you get 1)

10. when negating statements involving more quantifiers, each quantifier gets negated so that if it was $\exists$ it becomes $\forall$, and backwards. Don't forget to negate the $P(x,y)$ part that follows.

11. the negation of $\vee$ is $\wedge$, and the negation of $\wedge$ is $\vee$

12. the negation of $\geq$ is $<$, and similarly for the other inequality signs

13. **the negation of $p \to q$ is NOT $\neg p \to \neg q$.** But rather: the negation of $p \to q$ is the negation of $\neg p \vee q$ which is logically equivalent to $p \wedge \neg q$

1.5 Rules of Inference

Rules of Inference

1. an argument in propositional logic is a sequence of propositions that take the premise(s) to prove the conclusion(s) (an argument works for particular propositions)

2. an argument form in propositional logic is a sequence of propositions involving propositional variables that take the premise(s) to prove the conclusion(s) (an argument form is true no matter what particular propositions are used for the propositional variables, it is like a "rule" that works for all propositional variables used)

3. a rule of inference is a simple valid argument form that can be used as laws

4. rules of inference

   (a) law of detachment (modus ponens): $[p \wedge (p \to q)] \to q$

   (b) modus tollens: $[\neg q \wedge (p \to q)] \to \neg p$

(c) hypothetical syllogism: $[(p \to q) \wedge (q \to r)] \to (p \to r)$

(d) disjunctive syllogism: $[(p \vee q) \wedge \neg p] \to q$

(e) addition: $p \to (p \vee q)$ or similarly: $q \to (p \vee q)$

(f) simplification: $[p \wedge q] \to q$ or similarly $[p \wedge q] \to p$

(g) conjunction: $[(p) \wedge (q)] \to (p \wedge q)$ (if we know p and also q, then we have $p \wedge q$)

(h) resolution: $[(p \vee q) \wedge (\neg p \vee r)] \to (q \vee r)$

5. a fallacy of affirming the conclusion is an incorrect reasoning in proving $p \to q$ by starting with assuming q and proving p. For example: Show that if $x+y$ is odd, then either x or y is odd, but not both. A fallacy of affirming the conclusion argument would start with: "Assume that either x or y is odd, but not both. Then.."

6. a fallacy of denying the hypothesis is an incorrect reasoning in proving $p \to q$ by starting with assuming $\neg p$ and proving $\neg q$. For example: Show that if x is irrational, then $x/2$ is irrational. A fallacy of denying the hypothesis argument would start with: "Assume that x is rational. Then..."

Rules of Inference for Quantified statements

1. universal instantiation: knowing $\forall x, P(x)$ we can deduce $P(a)$ for any value a that we need.
   Example: Given that "For all irrational numbers x, we have that $\frac{x}{3}$ is irrational" prove that "$\frac{\sqrt{3}}{3}$ is irrational". To prove it, we note that $a = \sqrt{3}$ in our case, so letting $x = \sqrt{3}$ in $P(x)$, which is the statement "For all irrational numbers x, we have that $\frac{x}{3}$ is irrational". So if $x = \sqrt{3}$, then $\frac{\sqrt{3}}{3}$ is irrational, and the result follows.

2. universal generalization: knowing $P(a)$ for an arbitrary a we can deduce that $\forall x P(x)$ since a was arbitrary.
   Example: Given "Let a be an arbitrary irrational number. Then we have that $\frac{a}{3}$ is irrational." Prove that "For all irrational numbers x and y it is true that $\frac{x+y}{3}$ is irrational". To prove it, note that since $x + y$ is also irrational, we have that $\frac{x+y}{3}$ is

irrational, and in this case we generalized $P(a)$ to $P(x+y)$. (we will show that the sum of two irrationals is irrationals in the next section)

3. existential instantiation: knowing $\exists x, P(x)$ we can deduce $P(a)$ for some value a (sometimes you don't know the value of a but we know of its existence)
   Example: Given that "There is an irrational number x such that x^2 is also irrational" prove that "there is an irrational that can be written as a product of an irrational and a rational".

   To do so, we choose a to be an irrational such that a^2 is also irrational. Now construct the number $a+a$ which is still irrational, and so $(a+a)^2 = (2a)^2 = 4a^2$ is a number that is a product of the rational 4 and irrational a^2.

4. existential generalization: knowing $P(a)$ for some value of a we can deduce that $\exists x P(x)$ since there is at least one value for which it is true, for example the value a
   Example: Prove that there is a nonnegative number x such that $x^2 = x$. To prove it, we know that there is a value that verifies it, say $a = 1$. Since $P(1)$ it is true, we can thus say that $\exists x P(x)$.

1.6 Introduction to Proofs

1. a proof is a valid argument that establishes the truth of a theorem/proposition/lemma/corollary
2. an axiom (or postulate) is a statement that is assumed to be true without a proof
3. a conjecture is a statement that is being proposed to be true (usually based on partial results, intuition or heuristic argument) and it could become a theorem if it gets proved
4. Proof Methods in proving $P(x) \to Q(x)$ or equivalent statements
   (a) Direct Proof: *Assume $P(x)$ and prove $Q(x)$* (that's why it is the *direct* proof). The proof will generally start by choosing an arbitrary element (that is you can't assume anything particular about that element) of the domain, say a, (universal instantiation) and then proving the result about a. This far, we showed that $P(a) \to Q(a)$. Once this is done, since a was chosen arbitrary, we can then generalize it back and say that for $\forall x$ in the domain the result is T.
   (b) Contrapositive (Proof by Contraposition): *Assume $\neg Q(x)$ and prove $\neg P(x)$* (look at the truth tables to see that they are equivalent)
   (c) Vacuous Proof: In proving $P(x) \to Q(x)$ we find that *$P(x)$ is always F* for all values of x (so we get the implication: $F \to T/F$ which is always T)
   Example: If $x^2 \leq -2$, then x is even. (This is true since x^2 cannot be less than or equal to -2)

(d) Trivial Proof: In proving $P(x) \to Q(x)$ we find that *$Q(x)$ is always T* (without even using the given facts of $P(x)$).
Example: For positive numbers x, we have that $x^2 + 2 \geq 2$. (This is true no matter if x is positive or not)

(e) contradiction: we prove $P(x) \to Q(x)$ by proving that *$P(x)$ and $\neg Q(x)$ imply a contradiction*. Note that this is true since we are proving that if we assume $\neg(P(x) \to Q(x))$ we get a contradiction, which makes $P(x) \to Q(x)$ a tautology. To see this, observe that $\neg(P(x) \to Q(x)) \equiv \neg(\neg P(x) \vee Q(x)) \equiv P(x) \wedge \neg Q(x))$

5. Common mistakes:

(a) fallacy of affirming the conclusion (see section 1.5)

(b) fallacy of denying the hypothesis (see section 1.5)

(c) circular reasoning: a statement is proved using itself or a statement equivalent to it (see example 18 page 84)

1.7 Proof Methods and Strategy

1. The result is of the form $\forall x(P(x) \to Q(x))$ or equivalent statements

- Direct Proof: *assume $P(x)$ and prove $Q(x)$*
- Contrapositive: *assume $\neg Q(x)$ and prove $\neg P(x)$*
- Vacuous Proof: find that *$P(x)$ is always F* for all values of x
- Trivial Proof: find that *$Q(x)$ is always T* (without using $P(x)$).
- contradiction: prove that *$P(x)$ and $\neg Q(x)$ imply a contradiction*

within any of the above methods, one might have to use the following:

(a) proof by cases: if a single argument will not be valid for all values of x (every x of the domain needs to belong to one case). Cases should be considered if there is no obvious way to start a proof, since it may seem like not enough information is given in the hypotheses. The cases are usually given by the statement, depending on what the result says, however common cases are:

- (1) x is even and (2) x is odd
- (1) $x \geq 0$ and (2) $x < 0$ (sometimes $x = 0$ should be considered as Case (3))
- (1) $x \in \mathbb{Q}$ and (2) $x \notin \mathbb{Q}$

"WLOG" (Without loss of generality) should be used if two or more cases are similar, so that you wouldn't repeat the exact same proof.

(b) exhaustive proof: to prove the result, one may prove every possible example (that is if the number of examples is relatively small). It is not an elegant proof technique

2. Existence Proof: The result is of the form $\exists x(P(x) \to Q(x))$. Find one example α for which both $P(\alpha)$ and $Q(\alpha)$ are true. There are two forms of existence proofs:

   (a) constructive: when the value α is actually found

   (b) nonconstructive: when the existence of such value is proved, without specifying the value

3. Uniqueness Proof: The result is of the form $\exists!x(P(x) \to Q(x))$. It has two parts:

   - existence: show that there is an element (either constructive or not)
   - uniqueness: assume that there is another element, say $y \neq x$, and prove that either you get a contradiction or that $y = x$ (which is a contradiction as well)